Claims

What is claimed is:

1. A method for determining a level of trust in an authenticated identification, comprising:

performing at least one authentication to obtain an authentication result, each authentication having a score, each result indicating whether the corresponding authentication is successful; and

combining the scores for the successful authentications to determine a level of trust.

2. The method of claim 1, wherein performing at least one authentication comprises authenticating a purported identification.

3. The method of claim 1, wherein performing at least one authentication comprises authenticating a purported identification of one selected from the group consisting of a person, a document, and an item.

4. The method of claim 1, further comprising:

responsive to the determined level of trust exceeding a predetermined threshold, allowing access to a resource.

5. The method of claim 1, further comprising:

responsive to the determined level of trust exceeding a predetermined threshold, selecting a role for a user.

6. The method of claim 1, further comprising:

responsive to the determined level of trust exceeding a predetermined threshold, offering a user a role for selection.

7. The method of claim 1, further comprising:

responsive to the determined level of trust not exceeding a predetermined threshold, denying access to a resource.

8. The method of claim 1, further comprising:

responsive to the determined level of trust exceeding a first predetermined threshold, allowing a first level of access to a resource; and

responsive to the determined level of trust exceeding a second predetermined threshold, allowing a second level of access to a resource.

9. The method of claim 8, wherein each level of access corresponds to an allowed action with respect to the resource.

10. The method of claim 8, wherein the first level of access comprises reading the resource and the second level of access comprises modifying the resource.

11. The method of claim 4, 7, 8, 9, or 10, wherein the resource comprises a document.

12. The method of claim 1, further comprising:

receiving a request for an action, the action being associated with a predetermined minimum level of trust;

responsive to the determined level of trust exceeding the predetermined minimum level of trust, allowing the requested action to proceed; and

responsive to the determined level of trust not exceeding the predetermined minimum level of trust, denying the requested action.

13. The method of claim 1, further comprising:

presenting a list of allowable actions having minimum trust levels not exceeding the determined level of trust.

14. The method of claim 13, further comprising:

receiving input specifying one of the presented actions; and

initiating the specified action.

15. The method of claim 1, wherein combining the scores comprises determining a sum of the scores for the successful authentications.

16. The method of claim 1, wherein each authentication is performed according to an authentication method, and wherein the score for each authentication is associated with the corresponding authentication method.

17. The method of claim 16, where each authentication method is selected from the group consisting of:

password authentication;

secret question authentication;

smartcard authentication;

processor identification;

biometric identification; and

location identification.

18. The method of claim 1, wherein performing at least one authentication comprises determining a characteristic of a network connection.

19. The method of claim 18, wherein the determined characteristic of the network connection comprises a physical location of a computer connected via the network.

20. The method of claim 18, wherein the determined characteristic of the network connection comprises a degree of security associated with the network connection.

21. The method of claim 18, wherein the determined characteristic of the network connection comprises a previous authentication.

22. The method of claim 1, wherein each score indicates a relative degree of reliability of the corresponding authentication.

23. The method of claim 1, further comprising:

responsive to the determined level of trust, determining whether to allow or deny each of a plurality of requested actions during a user session.

24. A system for determining a level of trust in an authenticated identification, comprising:

an authenticator, for performing at least one authentication to obtain an authentication result, each authentication having a score, each result indicating whether the corresponding authentication is successful; and

a score combiner, coupled to the authenticator, for combining the scores for the successful authentications to determine a level of trust.

25. The system of claim 24, wherein performing at least one authentication comprises authenticating a purported identification.

26. The system of claim 24, wherein the authenticator authenticates a purported identification of one selected from the group consisting of a person, a document, and an item.

27. The system of claim 24, wherein the authenticator, responsive to the determined level of trust exceeding a predetermined threshold, allows access to a resource.

28. The system of claim 24, wherein the authenticator, responsive to the determined level of trust exceeding a predetermined threshold, selects a role for a user.

29. The system of claim 24, wherein the authenticator, responsive to the determined level of trust exceeding a predetermined threshold, offers a user a role for selection.

30. The system of claim 24, wherein the authenticator, responsive to the determined level of trust not exceeding a predetermined threshold, denies access to a resource.

31. The system of claim 24, wherein the authenticator, responsive to the determined level of trust exceeding a first predetermined threshold, allows a first level of access to a resource, and, responsive to the determined level of trust ex-

ceeding a second predetermined threshold, allows a second level of access to a resource.

32. The system of claim 31, wherein each level of access corresponds to an allowed action with respect to the resource.

33. The system of claim 31, wherein the first level of access comprises reading the resource and the second level of access comprises modifying the resource.

34. The system of claim 27, 30, 31, 32, or 33, wherein the resource comprises a document.

35. The system of claim 24, further comprising:

an action input device, couple to the authenticator, for receiving a request for an action, the action being associated with a predetermined minimum level of trust;

wherein the authenticator, responsive to the determined level of trust exceeding the predetermined minimum level of trust, allows the requested action to proceed, and, responsive to the determined level of trust not exceeding the predetermined minimum level of trust, denies the requested action

36. The system of claim 24, further comprising:

an output device, coupled to the authenticator, for presenting a list of allowable actions having minimum trust levels not exceeding the determined level of trust.

37. The system of claim 36, further comprising:

an input device, coupled to the output device, for receiving input specifying one of the presented actions; and

a transaction manager, coupled to the input device, for initiating the specified action.

38. The system of claim 24, wherein the score combiner determines a sum of the scores for the successful authentications.

39. The system of claim 24, wherein each authentication is performed according to an authentication method, and wherein the score for each authentication is associated with the corresponding authentication method.

40. The system of claim 39, where each authentication method is selected from the group consisting of:

password authentication;

secret question authentication;

smartcard authentication;

processor identification;

biometric identification; and

location identification.

41. The system of claim 24, wherein the authenticator performs at least one authentication by determining a characteristic of a network connection.

42. The system of claim 41, wherein the determined characteristic of the network connection comprises a physical location of a computer connected via the network.

43. The system of claim 41, wherein the determined characteristic of the network connection comprises a degree of security associated with the network connection.

44. The system of claim 41, wherein the determined characteristic of the network connection comprises a previous authentication.

45. The system of claim 24, wherein each score indicates a relative degree of reliability of the corresponding authentication.

46. The system of claim 24, wherein the authenticator, responsive to the determined level of trust, determines whether to allow or deny each of a plurality of requested actions during a user session.

47. A computer-readable medium for determining a level of trust in an authenticated identification, comprising:

computer-readable code adapted to perform at least one authentication to obtain an authentication result, each authentication having a score, each result indicating whether the corresponding authentication is successful; and

computer-readable code adapted to combine the scores for the successful authentications to determine a level of trust.

48. The computer-readable medium of claim 47, wherein the computer-readable code adapted to perform at least one authentication comprises computer-readable code adapted to authenticate a purported identification.

49. The computer-readable medium of claim 47, wherein the computer-readable code adapted to perform at least one authentication comprises computer-readable code adapted to authenticate a purported identification of one selected from the group consisting of a person, a document, and an item.

50. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust exceeding a predetermined threshold, allow access to a resource.

51. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust exceeding a predetermined threshold, select a role for a user.

52. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust exceeding a predetermined threshold, offer a user a role for selection.

53. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust not exceeding a predetermined threshold, deny access to a resource.

54. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust exceeding a first predetermined threshold, allow a first level of access to a resource, and, responsive to the determined level of trust exceeding a second predetermined threshold, allowing a second level of access to a resource.

55. The computer-readable medium of claim 54, wherein each level of access corresponds to an allowed action with respect to the resource.

56. The computer-readable medium of claim 54, wherein the first level of access comprises reading the resource and the second level of access comprises modifying the resource.

57. The computer-readable medium of claim 50, 53, 54, 55, or 56, wherein the resource comprises a document.

58. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to receive a request for an action, the action being associated with a predetermined minimum level of trust;

computer-readable code adapted to, responsive to the determined level of trust exceeding the predetermined minimum level of trust, allow the requested action to proceed, and, responsive to the determined level of trust not exceeding the predetermined minimum level of trust, deny the requested action.

59. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to present a list of allowable actions having minimum trust levels not exceeding the determined level of trust.

60. The computer-readable medium of claim 59, further comprising:

computer-readable code adapted to receive input specifying one of the presented actions; and

computer-readable code adapted to initiate the specified action.

61. The computer-readable medium of claim 47, wherein the computer-readable code adapted to combine the scores comprises computer-readable code adapted to determine a sum of the scores for the successful authentications.

62. The computer-readable medium of claim 47, wherein the computer-readable code adapted to perform at least one authentication performs each authentication according to an authentication method, and wherein the score for each authentication is associated with the corresponding authentication method.

63. The computer-readable medium of claim 62, where each authentication method is selected from the group consisting of:

password authentication;

secret question authentication;

smartcard authentication;

processor identification;

biometric identification; and

location identification.

64. The computer-readable medium of claim 47, wherein the computer-readable code adapted to perform at least one authentication comprises computer-readable code adapted to determine a characteristic of a network connection.

65. The computer-readable medium of claim 64, wherein the determined characteristic of the network connection comprises a physical location of a computer connected via the network.

66. The computer-readable medium of claim 64, wherein the determined characteristic of the network connection comprises a degree of security associated with the network connection.

67. The computer-readable medium of claim 64, wherein the determined characteristic of the network connection comprises a previous authentication.

68. The computer-readable medium of claim 47, wherein each score indicates a relative degree of reliability of the corresponding authentication.

69. The computer-readable medium of claim 47, further comprising:

computer-readable code adapted to, responsive to the determined level of trust, determine whether to allow or deny each of a plurality of requested actions during a user session.

70. A system for determining a level of trust in an authenticated identification, comprising:

authenticating means, for performing at least one authentication to obtain an authentication result, each authentication having a score, each result indicating whether the corresponding authentication is successful; and

score combining means, coupled to the authenticating means, for combining the scores for the successful authentications to determine a level of trust.

71. The system of claim 70, wherein the authenticating means, responsive to the determined level of trust exceeding a predetermined threshold, allows access to a resource.

72. The system of claim 70, wherein the authenticating means, responsive to the determined level of trust exceeding a predetermined threshold, selects a role for a user.

73. The system of claim 70, wherein the authenticating means, responsive to the determined level of trust exceeding a predetermined threshold, offers a user a role for selection.

74. The system of claim 70, wherein the authenticating means, responsive to the determined level of trust not exceeding a predetermined threshold, denies access to a resource.

75. The system of claim 70, wherein the authenticating means, responsive to the determined level of trust exceeding a first predetermined threshold, allows a first level of access to a resource, and, responsive to the determined level of trust exceeding a second predetermined threshold, allows a second level of access to a resource.